

# TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

## PCT

### RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM1414	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 03/02462	Date du dépôt international (jour/mois/année) 05/08/2003	(Date de priorité (la plus ancienne) (jour/mois/année) 09/08/2002
Déposant GEMPLUS		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

#### 1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).
3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

#### 4. En ce qui concerne le **titre**,

- ☐ le texte est approuvé tel qu'il a été remis par le déposant.
- ☒ Le texte a été établi par l'administration et a la teneur suivante:

PROCEDE DE CALCUL UNIVERSEL APPLIQUE A DES POINTS D'UNE COURBE ELLIPTIQUE

#### 5. En ce qui concerne l'**abrégi**,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant
- ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

#### 6. La figure des dessins à publier avec l'abrégi est la Figure n°

- ☒ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

1  
☐ Aucune des figures n'est à publier.

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 03/02462

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)  
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)  
EPO-Internal, PAJ

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
-------------	--	-------------------------------

X	<p>CHUDNOVSKY D V ET AL: "SEQUENCES OF NUMBERS GENERATED BY ADDITION IN FORMAL GROUPS AND NEWPRIMALITY AND FACTORIZATION TESTS"</p> <p>ADVANCES IN APPLIED MATHEMATICS, ACADEMIC PRESS, SAN DIEGO, CA, US, vol. 7, 1986, pages 385-434, XP008000716 ISSN: 0196-8858 page 418, dernier alinéa - page 424, alinéa 1</p> <p style="text-align: center;">----- -/--</p>	1-14
---	---	------

☒ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

9 mars 2004

Date d'expédition du présent rapport de recherche internationale

18/03/2004

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Verhoof, P

# RAPPORT DE RECHERCHE INTERNATIONALE

demande internationale No

PCT/FR 03/02462

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>BRIER E ET AL: "WEIERSTRASS ELLIPTIC CURVES AND SIDE-CHANNEL ATTACKS"                      5TH INTERNATIONAL WORKSHOP ON PRACTICE AND THEORY IN PUBLIC KEY CRYPTOSYSTEMS, PKC 2002, PARIS, FRANCE. LNCS 2274, 'Online! février 2002 (2002-02), pages 335-345, XP001068195                      Springer-Verlag, Berlin (DE)                      Extrait de l'Internet:                      URL: <a href="http://link.springer.de/link/service/series/0558/tocs/t2274.htm">http://link.springer.de/link/service/series/0558/tocs/t2274.htm</a>                      'extrait le 2002-02-05!                      cité dans la demande                      page 337, ligne 12 - page 340, ligne 4</p>	1,10-13
A	<p>JOYE M ET AL: "HESSIAN ELLIPTIC CURVES AND SIDE-CHANNEL ATTACKS"                      CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS CHES 2001. THIRD INTERNATIONAL WORKSHOP, PARIS, FRANCE, MAY 14-16, 2001, PROCEEDINGS. LNCS 2162,                      vol. 2162, 14 mai 2001 (2001-05-14), pages 402-410, XP008002643                      ISBN: 3-540-42521-7                      cité dans la demande                      page 395, ligne 8 - page 399, ligne 21</p>	1-10
A	<p>KHELDOUNI A ET AL: "Elliptic cohomology operation defined by Hecke operator T2"                      COMPTES RENDUS DES SEANCES DE L'ACADEMIE DES SCIENCES. SERIE I: MATHEMATIQUES, EDITIONS SCIENTIFIQUES &amp; MEDICALES ELSEVIER, FR,                      vol. 324, no. 2, janvier 1997 (1997-01), pages 215-220, XP004269356                      ISSN: 0764-4442                      page 216, ligne 12 - ligne 14</p>	1-14
T	<p>P. BARRETO ET AL.: "Constructing Elliptic Curves with Prescribed Embedding Degrees"                      SECURITY IN COMMUNICATION NETWORKS. THIRD INTERNATIONAL CONFERENCE, SCN 2002, AMALFI, ITALY, SEPTEMBER 11-13, 2002. REVISED PAPERS. LNCS 2576, 'Online! 2003, pages 257-267, XP002241906                      Springer Verlag, Berlin (DE)                      Extrait de l'Internet:                      URL: <a href="http://link.springer.de/link/service/series/0558/papers/2576/25760257.pdf">http://link.springer.de/link/service/series/0558/papers/2576/25760257.pdf</a>                      'extrait le 2003-03-14!                      page 259, dernier alinéa - page 260, alinéa 4</p>	1-14